Türk Telekom Siber Bülten

Aralık 2020

Türk Telekom Güvenlik

Türk Telekom
Değerli Hissettirir

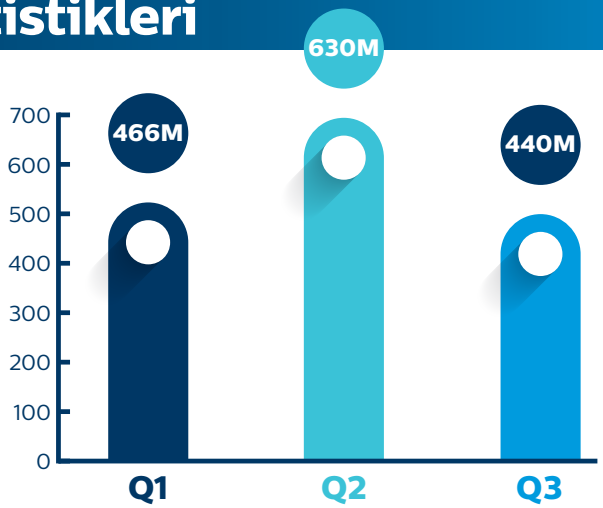
Gelişen teknolojiler ile birlikte siber saldırıların çeşitlendiği ve saldırganların dönemin açıklarına uygun farklı atak vektörlerini tercih ettiği görülmektedir. Bu ataklar bazen büyük şirketleri hedef alan ve ses getiren saldırılar olarak karşımıza çıkarken, bazen de bireysel kullanıcıları, küçük ve orta ölçekli işletmeleri hedef alan ve birçok kişinin saldırı gerçekleştikten çok sonra fark edebildiği ataklar olarak karşımıza çıkmaktadır.

İnternet üzerindeki işlem hacminin her geçen gün artması ve dijitalleşmedeki hızlı gelişiminin bir sonucu olarak, siber güvenlik her ölçekteki şirketin, şirket çalışanlarının ve bireysel kullanıcıların da önemsemesi gereken bir konu olarak karşımıza çıkmaktadır. Bu nedenle, farkındalığı arttırmak ve siber tehditlere karşı güncel kalmak amacıyla hazırladığımız bültenin bu sayısında saldırganların en sık kullandığı atak vektörlerinden bazılarını ve bu saldırılara karşı çözüm önerilerimizi bulabilirsiniz.

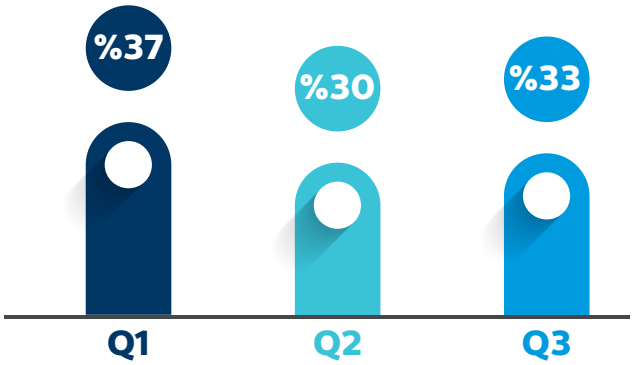
Türk Telekom Siber Atak İstatistikleri

Toplam Atak Sayıları:

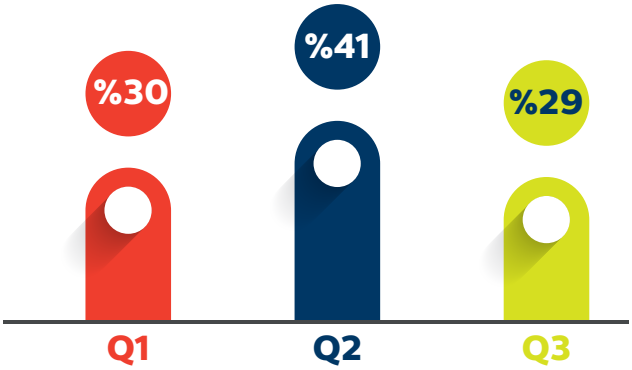
2020 üçüncü çeyrek verilerine göre atak trendlerinin çeyrek bazlı dağılımları gösterilmiştir.



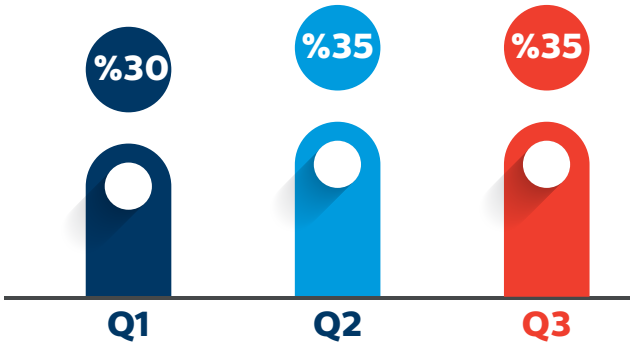
Gelişmiş Tehdit Önleme (APT):



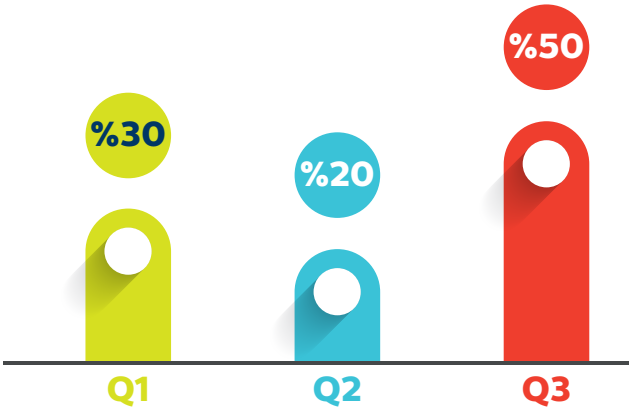
Aktif Savunma Sistemi (IPS):



Antivirüs Kategorisinde Engellenen Tehdit:

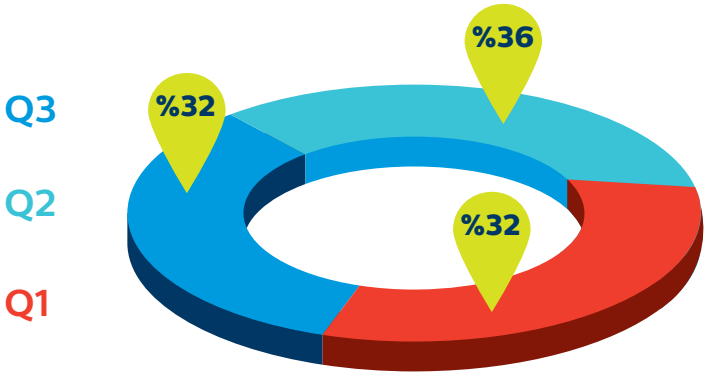


İçerik Filtreleme Engellenen Erişim:



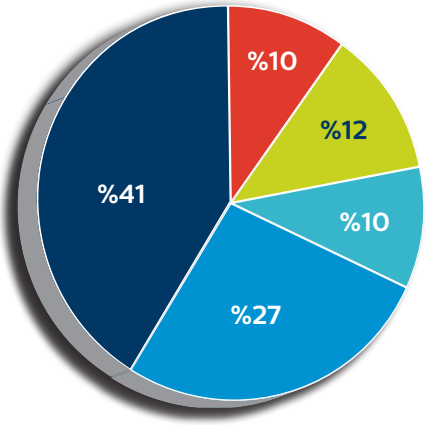
1 Gbps ve üzeri DDOS Atak Trendleri ve Sektör Dağılımları

DDOS Ataklarının Çeyrek Bazlı Dağılımı:



2020 YTD Verilerine Göre En Çok Atak Alan Sektörler

%41 Telekomünikasyon
%27 Veri Merkezleri
%12 Bilişim
%10 Kamu Kurum ve Kuruluşları
%10 Diğer



Siber Atak Vektörleri

1. DDOS Atakları– “NTP Amplifikasyon Saldırısı”

NTP amplifikasyonu, saldırganın hedeflenen UDP trafiğini aşmak için genel olarak erişilebilir Ağ Zaman Protokolü (NTP) sunucularından yararlandığı bir tür Dağıtılmış Hizmet Reddi (DDoS) saldırısıdır.

NTP istemcisi, NTP sunucusuna kendi saatini ekleyerek bir istek gönderir. NTP sunucusu kendi zamanı ve paketin geri gönderildiği zaman bilgisini NTP istemcisine döner. Bu işlem sonucunda, NTP istemcisi NTP sunucusunun saati ile kendi saati arasındaki zaman farkını hesaplayabilir. Çoğu ağ ortamında yerel cihazların saati yerel bir sunucuyla senkronize edilir. Yerel sunucu ise saatini güvenilir internet NTP sunucularıyla senkronize eder.

Saldırı Açıklaması:

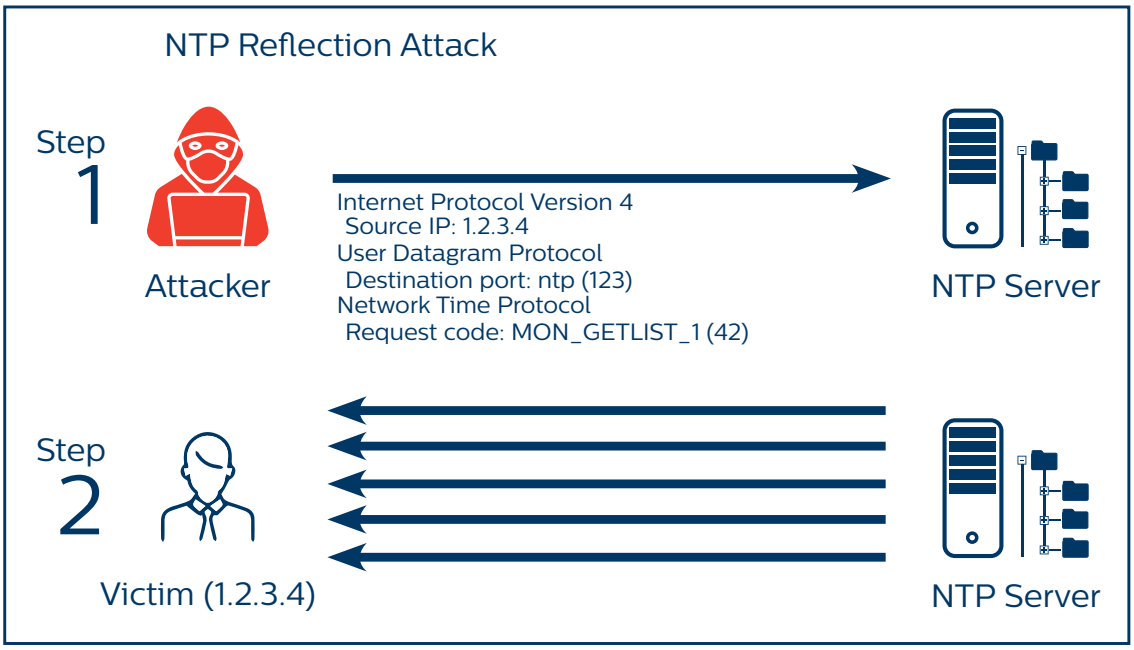
NTP amplifikasyonu aslında bir tür yansıma saldırısıdır. Yansıma saldırıları, bir sunucudan sahte bir IP adresine yanıt verilmesini içerir. Saldırgan, sahte IP adresine sahip bir paket gönderir ve sunucu bu adrese yanıt verir.

DNS amplifikasyon saldırılarında genellikle sorgu boyutu cevap boyutunun 70 katıdır. Bir NTP amplifikasyon saldırısında ise bu oran 20 kat, 200 kat ya da daha fazla olabilir. Bu da güncellenmemiş ve zafiyete açık NTP sunucularının listesini elde eden saldırganın kolayca yıkıcı boyutta yüksek hacimli bir DDoS saldırısı oluşturabileceği anlamına gelir.

NTP Amplifikasyon Saldırısı Nasıl Çalışır?

DDoS saldırılarında saldırganın amacı büyük miktarda ağ trafiği yaratarak, hedef sistemlerin karşılayabileceğinden daha fazla saldırı oluşturmaktır. Normal istekleri kullanarak bunu başarmak genellikle mümkün değildir bu nedenle saldırganın hedefe istek gönderen çok sayıda makineyi kontrol etmesi gerekir. DDoS saldırıları için kullanılan en yaygın ve en etkili tekniklerden biri yansıtma / büyütmedir. Saldırgan çok sayıda yanıtı kurbana yönlendirebilirse, az kaynakla çok zarar verebilir. DNS, SNMP v2 ve NTP gibi güvenlik açıklarına sahip birden çok protokol ve protokol uygulaması vardır. DNS, NTP gibi sunucular yüksek amplifikasyon faktörü nedeniyle saldırganlar tarafından daha çok tercih edilmektedir.

Siber Atak Vektörleri



Çoğu yansıma ve yükseltme zayıflığından yararlanmak için saldırganlar sahte IP kullanmaktadır. Aksi durumda NTP sunucusundan dönen yüksek hacimli cevap saldırgana geri iletilir.

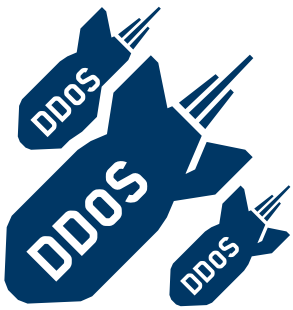
"NTP monlist" komutu kullanarak bir ağdaki monlist özelliği aktif olan diğer NTP sunucuları da tespit edilebilir. Ağınızda herhangi bir NTP sunucusu varsa ya da yoksa aşağıdaki maddeleri uygulayarak güvenlik korumanızı arttırabilirsiniz:

NTP sunucusu bulunuyorsa:
• NTP monlist komutu devre dışı bırakılmalıdır.
• NTP sunucusu bir güvenlik açığı tarayıcısıyla taranır ve güvenlik açığı algılanırsa NTP sunucusu için gerekli güncellemeler sağlanmalıdır.

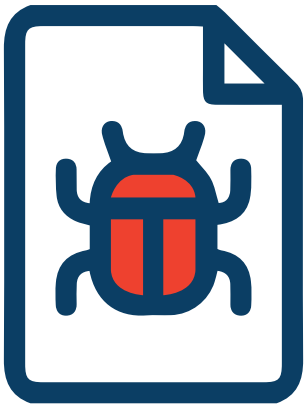
NTP sunucusu bulunmuyorsa:
• Sistemlerinize gelen NTP trafiğini izlenmelidir.
• Zaman senkronizasyonu gerekmiyorsa internete bakan varlıklarınızdaki UDP 123 portu kapatılmalıdır.

Her iki durumda da NTP amplifikasyon saldırılarına karşı ISP seviyesinde DDoS Atak Önleme çözümleriyle koruma sağlanabilir.

2020 üçüncü çeyreğinde Türk Telekom Anti-DDOS servisi tarafından tespit edilen DDoS alarmlarının %11'inin NTP Amplifikasyon tipinde olduğu görülmüştür.



2. Zararlı Yazılımlar



«Dekont.xls » Zararlı Dosya İncelemesi

Şüpheli dosya, içerisinde Excel 4.0 macrolarına (XML) sahip olup, dosya çalıştırıldığında otomatik olarak zararlı aktivite gerçekleştiren bir kod içerdiği saptanmıştır. Detaylı olarak analiz sonuçlarına göre aşağıdaki bulgulara rastlanılmıştır:

1- URL'in tehdit istihbaratı kaynaklarında C&C IOC IP'lerinden biri olduğu görülmüştür.

2- Zararlı yazılımın daha sonra standart olmayan port 8808 aracılığıyla [185.140.53.48 IP adresine sahip sunucu ile iletişime geçtiği saptanmıştır. İlgili IP adresi ile ilişkili birçok zararlı yazılımın olduğu ve bu IP adresine sahip domain kayıtlarının olduğu tespit edilmiştir.

3. Web Uygulama Atakları

Kimlik Bilgisi Doldurma (Credential Stuffing), saldırganın güvenliği ihlal edilmiş kimlik bilgilerini web uygulamalarında, oturum açma sayfalarına enjekte ederek kullanıcı hesaplarına erişim sağlamaya çalıştığı bir saldırı çeşidir.
Saldırganlar genellikle bu bilgileri popüler web sitelerine saldırı başlatmak amacıyla toplamaktadırlar.
Bu saldırılarda, bilgisayar korsanları veri ihlalleri veya başka yollarla sızdırılan kimlik bilgilerini alır ve ardından bu kimlik bilgilerini bir kullanıcının diğer hesaplarında oturum açmak için kullanmayı amaçlarlar. Veri ihlalinden elde edilen kimlik bilgileri bankacılık sitesi gibi başka bir sitede yeniden kullanılırsa, saldırgan kullanıcının banka hesabına erişim sağlayıp işlem gerçekleştirebilir.
Yapılan araştırmalar kullanıcıların % 83'ünün birden fazla sitede aynı şifreyi kullandığını ortaya çıkarmıştır.

Kimlik bilgisi doldurma saldırısı, 2018'de 30 milyar deneme kaydetmesiyle oldukça yaygın bir saldırı türü haline gelmiştir. Bugün ise, saldırı sayılarının her gün ortalama 115 milyon denemeye ulaştığı görülmektedir.

Genellikle kaba kuvvet saldırıları ve kimlik bilgisi saldırılarının aynı olduğu düşünülür ancak kimlik bilgilerini doldurma daha farklıdır. Kaba kuvvet saldırıları, bazen genel parola önerileriyle birlikte rastgele karakterler kullanarak deneme yanılma yöntemi ile parolaları tahmin etmeye çalışır. Kimlik bilgisi doldurma saldırısında ise daha önceden ele geçirilmiş kimlik bilgileri kullanılarak saldırı gerçekleştirilir.
Kimlik bilgilerini doldurma saldırılarının tespit edilmesi ve engellenmesi çok daha zordur. Çünkü bunlar, tek bir hesap için tekrarlanan oturum açma girişimlerinden ziyade çok sayıda farklı hesapta oturum açmaya yönelik dağıtılmış girişimleri içerir.

Kimlik Bilgisi Doldurma Saldırıları için öneriler:
- Kullanılmayan çevrimiçi hesapların kapatılması ya da silinmesi
- Aktif hesaplarda aynı parolanın kullanılmaması
- Güvenli bir şifre kullanılarak düzenli olarak değiştirilmesi
- İki faktörlü kimlik doğrulamanın etkinleştirilmesi

Web sitenize yönelik bu tür saldırılardan korumak için Türk Telekom WAF servisinden faydalanabilirsiniz.

1. Türk Telekom WAF (Web Uygulama Güvenlik Duvarı)

Web uygulama güvenlik duvarı(WAF), web uygulamalarında güvenlik tehdidi oluşturabilecek, erişilebilirliğini etkileyecek zararlı içeriklere ve web sitelerindeki açıklara karşı koruma sağlayan bir servistir. Uygulama katmanında görev alır ve son kullanıcı ile web sunucuları arasında oluşan iletişimi dinleyerek otomatik ya da kurumlara özel tanımlanan kurallar kapsamında filtreleme, düzeltme yapar ve güvenlik tehditlerini engeller.

Web Uygulama Güvenlik duvarı, karmaşıklaşan web trafiği üzerinde detaylı inceleme yaparak anormal trafiği engellemeye yarayan teknolojidir. HTTP/HTTPS/SOAP/XML/ Web servisleri üzerinde detaylı paket incelemesi yaparak zararlı istekleri bloklamak için kullanılan bir araçtır.

Açık web uygulama güvenliği projesi anlamına gelen OWASP, güvensiz yazılımların oluşturduğu problemlere karşı mücadele etmek için kurulmuş bir topluluktur.

OWASP'ın listesine göre web uygulamalarında bulunan zafiyetlerinden birkaçı şu şekildedir:

- **SQL Injection;** Kod enjeksiyon saldırıları, kullanıcılardan gelen dataların kontrol edilmeden komutlarda veya veri tabanı sorgularında kullanılmasıyla meydana gelir.
- **CrossSiteScript;** CrossSiteScripting, saldırganın zararlı kodlarını web uygulamasına dahil etmesidir, bu kodlar uygulamayı ele geçirmeye kadar gidebilir.
- **Cross Site Request Forgery;** CSRF açıkları, gelen taleplerde oturum kontrolü yapılmasının unutulması nedeniyle gerçekleşir.
- **Broken Authentication and Session Management;** Web uygulaması, kullanıcıları tanımlamak için oluşturduğu sessionID'lerini cleartext veya kolay kırılabilir bir şifreleme ile oluşturuyorsa meydana gelen bir zafiyettir.
- **Insecure Cryptographic Storage;** Veri tabanı sistemlerinde, hassas bilgilerin şifrelenmeden tutulması durumunda oluşmaktadır.
- **Using Components with Known Vulnerabilities;** Bilinen güvenlik açıklarına sahip bileşenleri kullanan uygulamalar ve API'ler, uygulama savunmalarını zayıflatabilir ve çeşitli saldırılara kapı açabilir.

Türk Telekom WAF hizmeti, global ve yerli çözümlerle hem coğrafi hem de marka yedekli yapısı ile ilk andan itibaren uygulamalarınızı siber saldırılara karşı korumaktadır.

Türk Telekom Ürün ve Servisleri

Türk Telekom WAF (Web Uygulama Güvenlik Duvarı)

Türkiye'nin ilk yönetimli WAF hizmetini sunan servis sağlayıcısı olarak müşterilerimize;

- Yönetimli ve yönetimsiz alternatiflerle uygulama güvenliği sunmaktayız.
- Gelişmiş yük dengeleme, dosya zararlı yazılım taraması, Owaps 10, ve global tehdit istihbaratı gibi birçok entegre özelliğin yanı sıra yönetim portali ve anlık raporlama imkanı da sağlamaktayız.
- Erişim bağımsız sunulan WAF servisinde, uygulama trafik boyutuna göre ücretlendirilen esnek ve uygun aylık tarife modeli ile bu hizmetten faydalanabilirsiniz.

2. McAfee Total Protection ile Uç Cihaz Güvenliği

Türk Telekom Mcafee Total Protection hizmeti antivirüs, güvenlik duvarı, spam filtresi, kötü amaçlı URL engelleme, dosya şifreleme, parola yöneticisi, güvenli dosya silme, uygulama, web performansı artırıcılar ve temel kimlik hırsızlığı koruması içeren gelişmiş güvenlik paketidir. Sıfırıncı gün kötü amaçlı yazılım saldırılarına karşı Total Protection, saldırıları tespit eder ve engeller. Türk Telekom mobil ve internet müşterilerine sunulan Mcafee Total Protection ile PC, MAC, akıllı telefon ve tabletleri için mutlak güvenlik koruması sağlar.
Dünya çapında 325 milyon cihazı koruyan Mcafee Total Protection; AV-TEST'in performans değerlendirmesi 6/6 dır ve Windows, Android, MacOS ve IOS işletim sistemleri için uyumludur.

Özellikler:

Zararlı yazılımları algılar	Yeni tehditleri anında analiz ederek milisaniyeler mertebesinde engelleme
Hızlı ve etkin tarama	Hızlı ve etkin virüs, zararlı yazılım ve casus yazılım taramalarıyla en az düzeyde kesinti ile çalışma
Kesintisiz tarama	Otomatik taramalar ve güncellemeler bilgisayar boşta iken yapılır.
Akıllı uyarılarla güvenlik durumunu kolay yönetme	Kullanımı kolay, uyarı sistemleri ve anlaşılması ile önemli ürün uyarıları sağlar.
Site Advisor ile webde daha güvenli gezinme	Olası zararlı web sitelerini tanıma özelliği sayesinde daha güvenli internet araması, gezintisi ve alışverişi sağlar.
QuickClean ile daha sağlıklı bilgisayar	QuickClean ile performansı etkileyecek gereksiz dosyaları kaldırır.
Shredder ile dijital dosyaları tamamen ortadan kaldırma	Shredder aracıyla dijital dosyaları daha sonra erişilmesini engellemek için parçalar.
Anti-spam ve e-posta koruma	Gelişmiş SPAM tanıma özelliği ile gelen kutunuzdaki tıkanmaları önler.
Gelişmiş Ebeveyn Denetimleri ile Çocuk Koruma	Gelişmiş Ebeveyn Denetimleri ile Çocuk Koruma sağlar.

Tehdit İstihbaratı Verileri

1. Şüpheli IP Adresleri

171[.]25[.]193[.]77	51[.]158[.]111[.]157	24[.]207[.]90[.]159	195[.]176[.]3[.]20	45[.]95[.]168[.]150	111[.]161[.]66[.]250
54[.]38[.]81[.]231	128[.]31[.]0[.]13	118[.]126[.]105[.]120	175[.]24[.]72[.]167	106[.]12[.]60[.]40	45[.]95[.]168[.]150
145[.]239[.]252[.]197	54[.]36[.]108[.]162	151[.]80[.]16[.]169	111[.]231[.]77[.]115	139[.]59[.]116[.]115	106[.]12[.]60[.]40
51[.]15[.]43[.]205	150[.]129[.]8[.]34	194[.]180[.]224[.]103	87[.]98[.]156[.]136	175[.]24[.]59[.]130	139[.]59[.]116[.]115
51[.]75[.]144[.]58	185[.]117[.]215[.]9	80[.]82[.]70[.]118	195[.]154[.]179[.]3	62[.]234[.]126[.]132	175[.]24[.]59[.]130
87[.]98[.]152[.]111	164[.]132[.]51[.]91	185[.]220[.]102[.]253	94[.]102[.]49[.]193	193[.]112[.]93[.]94	185[.]220[.]101[.]215
185[.]213[.]155[.]169	178[.]73[.]215[.]171	185[.]220[.]102[.]252	124[.]206[.]0[.]224	118[.]194[.]132[.]112	185[.]220[.]101[.]212
171[.]25[.]193[.]20	150[.]129[.]8[.]19	185[.]220[.]102[.]251	167[.]99[.]170[.]91	42[.]123[.]99[.]67	185[.]220[.]101[.]213
51[.]77[.]135[.]89	50[.]234[.]173[.]102	185[.]220[.]102[.]250	150[.]109[.]52[.]213	107[.]187[.]122[.]10	37[.]49[.]224[.]154
185[.]220[.]102[.]254	185[.]220[.]102[.]249	51[.]79[.]86[.]177	118[.]25[.]14[.]19	185[.]220[.]100[.]252	192[.]144[.]186[.]22
87[.]98[.]155[.]50	212[.]47[.]229[.]4	185[.]220[.]101[.]144	164[.]68[.]112[.]178	104[.]236[.]115[.]5	185[.]220[.]101[.]11
217[.]182[.]194[.]103	167[.]88[.]7[.]134	150[.]129[.]8[.]24	150[.]129[.]8[.]31	116[.]228[.]37[.]90	46[.]101[.]40[.]21
51[.]75[.]52[.]118	150[.]129[.]8[.]32	150[.]129[.]8[.]28	106[.]124[.]136[.]103	165[.]22[.]143[.]3	208[.]68[.]39[.]124
87[.]98[.]152[.]54	104[.]244[.]77[.]95	89[.]248[.]167[.]131	51[.]91[.]100[.]120	185[.]107[.]70[.]202	106[.]54[.]242[.]239
85[.]209[.]0[.]103	145[.]239[.]92[.]26	94[.]142[.]244[.]16	164[.]52[.]24[.]168	45[.]15[.]16[.]100	118[.]116[.]8[.]215
51[.]38[.]10[.]45	162[.]247[.]74[.]201	185[.]220[.]101[.]13	210[.]105[.]148[.]87	159[.]203[.]74[.]227	185[.]220[.]101[.]196
178[.]32[.]123[.]182	171[.]25[.]193[.]78	150[.]129[.]8[.]8	159[.]89[.]129[.]36	134[.]209[.]250[.]37	163[.]172[.]125[.]41
89[.]234[.]157[.]254	185[.]220[.]101[.]3	162[.]247[.]73[.]192	161[.]35[.]60[.]51	185[.]10[.]68[.]152	172[.]81[.]253[.]233
217[.]182[.]192[.]217	18[.]27[.]197[.]252	195[.]206[.]105[.]217	140[.]246[.]182[.]127	211[.]103[.]183[.]3	185[.]220[.]101[.]138
51[.]77[.]52[.]11	217[.]170[.]205[.]14	79[.]137[.]79[.]167	185[.]220[.]103[.]7	198[.]251[.]89[.]80	89[.]236[.]112[.]100
185[.]220[.]103[.]5	89[.]144[.]12[.]17	62[.]210[.]105[.]116	192[.]3[.]255[.]139	185[.]170[.]114[.]25	51[.]83[.]139[.]56
192[.]42[.]116[.]24	162[.]247[.]72[.]199	195[.]54[.]160[.]183	185[.]107[.]47[.]171	157[.]245[.]142[.]218	193[.]56[.]28[.]186
178[.]32[.]124[.]62	185[.]220[.]100[.]253	185[.]100[.]87[.]206	185[.]220[.]101[.]4	162[.]247[.]74[.]216	193[.]112[.]100[.]92
178[.]32[.]123[.]204	87[.]98[.]154[.]134	185[.]100[.]87[.]207	185[.]220[.]101[.]1	195[.]144[.]21[.]219	185[.]220[.]103[.]8
178[.]32[.]123[.]203	185[.]165[.]168[.]229	45[.]14[.]150[.]130	104[.]248[.]16[.]41	82[.]64[.]15[.]106	185[.]220[.]103[.]6
51[.]75[.]64[.]187	150[.]129[.]8[.]4	110[.]45[.]155[.]101	89[.]31[.]57[.]5	94[.]102[.]51[.]78	46[.]101[.]33[.]198
150[.]129[.]8[.]5	211[.]65[.]196[.]105	85[.]209[.]0[.]101	157[.]230[.]245[.]91	104[.]248[.]126[.]170	122[.]51[.]81[.]247
54[.]38[.]75[.]44	54[.]38[.]75[.]41	80[.]82[.]77[.]33	206[.]189[.]127[.]6	185[.]220[.]101[.]21	185[.]100[.]85[.]61
145[.]239[.]7[.]56	54[.]38[.]75[.]42	137[.]74[.]169[.]241	144[.]217[.]42[.]212	192[.]42[.]116[.]16	76[.]72[.]169[.]18
185[.]220[.]102[.]8	87[.]98[.]156[.]62	148[.]70[.]18[.]216	112[.]116[.]155[.]205	64[.]225[.]46[.]17	139[.]220[.]192[.]57
77[.]247[.]181[.]165	185[.]130[.]44[.]108	64[.]225[.]47[.]162	67[.]205[.]162[.]223	157[.]245[.]154[.]123	112[.]70[.]191[.]130
51[.]195[.]148[.]18	51[.]255[.]77[.]78	165[.]22[.]40[.]147	109[.]69[.]67[.]17	167[.]172[.]38[.]238	218[.]17[.]162[.]119
209[.]141[.]45[.]189	193[.]218[.]118[.]131	94[.]102[.]49[.]7	159[.]89[.]224[.]99	155[.]4[.]117[.]13	134[.]209[.]164[.]184
176[.]10[.]104[.]240	51[.]178[.]52[.]245	92[.]62[.]136[.]213	185[.]162[.]235[.]222	51[.]210[.]34[.]150	222[.]186[.]42[.]7
87[.]98[.]152[.]180	37[.]49[.]224[.]156	51[.]15[.]80[.]14	129[.]226[.]117[.]160	164[.]132[.]145[.]70	165[.]22[.]77[.]163
178[.]33[.]42[.]215	85[.]248[.]227[.]165	150[.]129[.]8[.]33	185[.]220[.]101[.]46	87[.]98[.]156[.]68	171[.]25[.]193[.]25
51[.]83[.]69[.]84	185[.]220[.]101[.]12	222[.]186[.]30[.]218	116[.]236[.]2[.]254	185[.]220[.]102[.]6	138[.]68[.]94[.]142
185[.]212[.]168[.]245	77[.]247[.]181[.]162	192[.]241[.]246[.]167	142[.]93[.]130[.]58	185[.]220[.]102[.]7	145[.]239[.]7[.]78
36[.]67[.]200[.]85	138[.]68[.]81[.]162	109[.]70[.]100[.]26	61[.]161[.]250[.]202	68[.]183[.]137[.]173	47[.]241[.]10[.]157
87[.]98[.]139[.]44	178[.]32[.]125[.]162	106[.]13[.]41[.]25	80[.]82[.]77[.]139	120[.]133[.]1[.]16	64[.]227[.]26[.]221
178[.]32[.]123[.]99	185[.]220[.]102[.]4	159[.]65[.]224[.]137	71[.]6[.]146[.]186	153[.]101[.]29[.]178	162[.]247[.]74[.]7
178[.]32[.]124[.]74	87[.]98[.]151[.]169	38[.]95[.]167[.]16	106[.]13[.]56[.]204	93[.]157[.]62[.]102	178[.]62[.]49[.]137
51[.]75[.]144[.]43	193[.]228[.]91[.]108	51[.]79[.]53[.]139	80[.]82[.]65[.]90	104[.]248[.]63[.]105	64[.]225[.]102[.]53
54[.]39[.]16[.]73	193[.]228[.]91[.]109	47[.]241[.]26[.]71	94[.]230[.]208[.]147	120[.]53[.]10[.]191	208[.]68[.]39[.]220
145[.]239[.]1[.]182	217[.]170[.]206[.]138	64[.]225[.]70[.]13	23[.]129[.]64[.]203	150[.]129[.]8[.]27	203[.]236[.]51[.]35
194[.]180[.]224[.]130	145[.]239[.]82[.]87	160[.]124[.]50[.]93	178[.]20[.]55[.]16	193[.]218[.]118[.]130	
185[.]220[.]101[.]207	176[.]10[.]99[.]200	91[.]121[.]175[.]61	103[.]123[.]65[.]35	138[.]197[.]89[.]212	
87[.]98[.]155[.]123	158[.]69[.]35[.]227	106[.]13[.]49[.]133	111[.]161[.]66[.]250	139[.]59[.]57[.]2	

2. Oltalama Saldırısı için Oluşturulmuş Domain Bilgileri

"sargento-usa[.]com",	"localbitcoins-airdrop-program[.]receipt-wi-rexapp[.]com",	"ucb[.]globalsecured[.]top",
"etoro-mining[.]co",	"localbitcoinse[.]net",	"ucb[.]wbsecured[.]top",
"proetoro[.]com",	"localbitcoins[.]ru[.]net",	"paxoceans[.]com",
"xn--localbitcns-yeb49e[.]com",	"transnetboxing[.]co[.]za",	"www[.]cambridgecbgroup[.]online",
"xn--localbitcons-8j6f[.]com",	"vistratfonline[.]com",	"us[.]ucbintl[.]top",
"minterellison[.]co",	"bitstarz-casino-2020[.]ru",	"bitstarzmovies[.]online",
"www[.]e-blockinvest[.]com",	"bitstarz28-casino[.]ru",	"localbitcoins[.]center",
"ietoro[.]com[.]tw",	"casinobitstarz[.]com",	"bitstarz-promo[.]org",
"etoroinvestment[.]org",	"bitstarzcasinoreview[.]ru",	"diversifiedsus[.]com",
"lionsqate[.]com",	"bitstarz-casino-new[.]ru",	"weatherbycs[.]com",
"localbiencins[.]com",	"localbtccoins[.]com",	"myetherwallet[.]keynasty[.]com",
"minter-ellison[.]com",	"localbitcoins[.]me",	"domainpostmaster[.]email",
"minterellison[.]org",	"ibb[.]hh-kunde[.]de",	"mimecast[.]domaincontrol7[.]com",
"cevaexpress[.]com",	"app[.]mmlgax[.]com",	"login-mimecast[.]maxxis[.]ee",
"postmaster--eu[.]protection-mimecast[.]laco-medialocal[.]com",	"etoroglobal[.]us",	"www[.]mytiethervveallet[.]com",
"xn--localbitoins-rdb[.]com",	"pronline[.]anjl-ceva[.]com",	"bitstarz-casino[.]su",
"xn--lcalbtcons-o8ad3e[.]net",	"localsbitcoin[.]net",	"www[.]cambridgecb[.]online",
"xn--localbtcns-p8ac1f[.]net",	"bitstarz-casino14[.]ru",	"lmax[.]pro",
"www[.]aytekinyapi[.]com",	"zynecoin[.]io[.]imported-myetherwallet[.]com",	"localbitcoins-accounts-logins[.]consultasar-gentinas[.]com",
"posmaster--eu[.]protection-mimecast[.]thank-fullyorganized[.]com",	"cambridgecb[.]digital",	"localbitcoins[.]com[.]accounts-login[.]perso-nas-banmochile[.]com",
"postmaster--eu[.]protection-mimecast[.]yaseenmustafa[.]net",	"develop[.]mewbuilds[.]com",	"myehterwaltet[.]com",
"localbitics[.]ru",	"myethwallet[.]org",	"xn--ve-localbtcoins-dpb[.]com",
"minterellison[.]xyz",	"playbitstarz[.]net",	"xn--ve-localbtcons-8lbd[.]com",
"mimecastit[.]weebly[.]com",	"muetherwallet[.]co",	"xn--log-localbtcoins-isb[.]com",
"etoro-invest[.]org",	"myetherwallet[.]com[.]get-coin-erc20-mem-ber[.]com",	"imprviata[.]com",
"cevalogisticsonline[.]com",	"aoncology[.]net",	"xn--logln-localbtcoins-syb[.]com",
"velvetbank[.]online",	"lmaxtrade[.]com",	"localbitcoins[.]trustedonlinetradeoptions[.]com",
"royalfinancebank[.]online",	"myetherwallet[.]com[.]icotoken[.]digital",	"localbniscoins[.]live",
"mimeecast[.]weebly[.]com",	"pcfsaving[.]com",	"eazypaybtc[.]com",
"paccoffshoresg[.]com",	"c6ir6kp1[.]global-lmax[.]com",	"ioatradefx[.]com",
"mmimecast[.]weebly[.]com",	"ucb[.]edirectonline[.]com",	"cevaloglstics[.]com",
"lmaxhk[.]com",	"eon[.]hu[.]e-portal[.]pbonlinemarketingser-vices[.]com",	"underlivering-messages-375246156mime-cast[.]gasbookingagency[.]in",
"mimecastdev[.]myservicenow[.]io",	"unimel-edu[.]org",	"xn--slgn-localbtcoins-nvb[.]com",
"mcgoughc[.]com",	"ucb[.]eonlineaccess[.]com",	"slgn-localbltcoins[.]com",
"etoroinvest[.]org",	"ettoro[.]org",	"sign-localbltcoins[.]com",
"sargentorewards[.]com",	"myetharwallets[.]com",	"localbincons[.]com",
"etoroglobaltrade[.]com",	"myetherwallet-inc[.]com",	"localbencoins[.]com",

3. Oltalama Saldırısı için Oluşturulmuş URL Ardesleri

"https://etorotradeforex[.]net/trade/",	"http://bankhapoalimus[.]com/bhi-connect-login/login[.]php",
"http://xn--logn-localbtcoins-wubi[.]com/accounts/login/",	http://www[.]expressdoner[.]pl/wordpress/wp-includes/js/tinymce/utils/cast/
"https://darlanmendoza[.]com/Mimecast/Mimecast%20Errors/login[.]php",	"https://notre-courtier[.]fr/wp-includes/css/dist/nux/login[.]mimecast[.]com[.]html",
"https://2050391180620948717180[.]us-south[.]cf[.]appdomain[.]cloud/mimeief4OLVfRFm/mimeief4OLVfRFm[.]php",	"https://localbitcoins[.]sale/reply/",
"http://www[.]atlantiscity1konutlari[.]com/wp-content/plugins/caitlyn/au/aaf5eefbf0cce0afd500044f61bd7f9c/",	"http://cutt[.]us[.]com/3UeFXMP",
"http://mail[.]goyak[.]com/language/il/",	"https://rmyelhervvalellet[.]com/Send",
"http://mail[.]goyak[.]com/mail/help/my-account/dir/files/86e4d847bfd0e3ba2c2c5094fc1c12f5/index[.]html",	"https://www[.]myelhearvvlellat[.]com/M/Y/",
"https://www-cwbank[.]com/en/business",	"https://globalweatherbys[.]com/en/",
"http://217[.]128[.]48[.]188:32000/mail/lang/il/",	"http://login-mimecast[.]magnuspost[.]com[.]au/auth/",
"http://lstlambert-658-1-140-188[.]w217-128[.]abo[.]wanadoo[.]fr:32000/mail/lang/il",	"http://login-mimecast[.]erotikboudoir[.]xyz/auth/",
"https://www[.]facebook[.]com/PumaPay-110515940736460/",	"https://etoroglobal[.]us/login",
"http://akinsoft[.]org:32000/webmail/skins/il/29af3a00d9d037b0206a32c5e4eff45d/",	"https://www[.]youtube[.]com/channel/UCNBETVFIIM-WH4ePq9qRVUVg",
"http://210[.]1[.]51[.]166:32000/mail/lang/fr2/",	"http://rewards-program-erc-20-token[.]com/myetherwallet[.]html?/access-my-wallet",
"http://ns15[.]4gbhost[.]com:32000/mail/lang/fr2"	"http://ucb[.]53international[.]icu/ibanksecure/",
"https://www[.]linkedin[.]com/in/limor-ferber-07b367103/",	"http://zynecoin[.]io[.]connected-myetherwallet[.]com/connected-MyEtherWallet[.]php",
"http://u796594eme[.]ha004[.]t[.]justns[.]ru/diana/hapolim2/",	"http://vdkbankbe[.]be[.]onlinebankieren[.]info/aanvraag/",
"http://82[.]166[.]42[.]244:32000/accounts/lang/il",	"http://localbitcoins[.]com-anti-money-laundering[.]contact-our-support[.]com/login[.]html",
"http://mail[.]s2otomasyon[.]com:32000/webmail/server/il/ef98637eeae7713e894bd5dfdd2b8647/index[.]html",	"https://automotrizoregon[.]cl/mime/login[.]php",
"http://bit[.]ly/3gLPW9D",	"https://localbitcoins[.]com-anti-money-laundering-policy[.]open-tickets[.]com/login[.]html",
"https://android-top[.]com/apk/com[.]mimecast",	"https://qcoregroup[.]com/PROPERTY/u/login/index[.]php",
"http://banh[.]com:8080/accounts/lang/il",	"https://amateurhourradiostl[.]com/mimcast/u/login/erb[.]php",
"http://191[.]236[.]36[.]79:8080/accounts/lang/il/314e8acaa9a76f5beca0eb5372dbad82/index[.]html",	"https://amateurhourradiostl[.]com/mimcast/u/login/era[.]php",
"https://lhodgebuk[.]com/en/index[.]html",	"http://35[.]188[.]36[.]185/mimecast/27-03-2020/portal[.]mimecast[.]com/website/index[.]html",
"http://bit[.]ly/2O4hU3X",	"https://toabroad[.]com/mimcast/u/login/index[.]php?email=kokowawa",
"http://bit[.]ly/3gmJaXM",	"http://app-mimecast[.]salience[.]ae/auth",
"http://mail[.]sterilite[.]net/accounts/lang/il/4a448122990309d1d7a6b266e455498c/index[.]html",	"https://postmaster[.]asia/auth",
"http://68[.]67[.]33[.]214/accounts/il/58eaf2c67e2cbe5fa8e3bd32a20ea711/index[.]html",	"https://protection-mimecast[.]mateszalkaiszc[.]hu/auth/?user=",
"https://bit[.]ly/2Zx2fzz",	"http://salienceconsulting[.]ae/regulatory",
"http://68[.]67[.]33[.]214/accounts/il/7ade71af4c00e4d9a87db98b682259b8/index[.]html",	"http://mimecast[.]postmaster[.]asia/auth/",
"http://mail[.]tothenextlevel[.]com/accounts/lang/il/",	"http://protection-mimecast[.]tchebagaul[.]com/auth/",
"https://www[.]bitstarz[.]ca/www[.]bitstarz[.]com/",	"http://mimecast[.]tchebagaul[.]com/auth/",
"http://forexsq[.]com/etoro-review/",	"https://profiloturkiye[.]com/mimecast/mimecast/mimecast/clog-in[.]php",
"https://allmaart[.]com/wp-includes/Text/pin/mime[.]com/cast/",	"https://elrond[.]com[.]erc20-gift-token[.]com/Error[.]MyEtherWallet[.]html?/import_PrivateKey_or_phrase_claim_bonus",
"http://datalakewonder[.]com:32000/mail/lang/il/43cc903105d274dd1256ba5cbe5f44cc/index[.]html",	"https://rebrand[.]ly/uqhmirs",
"http://bit[.]ly/2NBV9UM",	"https://email[.]secureto[.]com/admin/temp/forms/dnr/diners/signin[.]php?country=IL-Israel&lang=en",
"http://103[.]25[.]130[.]114/easycontact/link[.]php?M=2661&N=16&L=6&F=H",	"https://www[.]myatharweiiect[.]com/vlc/?xfsr=true"
"https://mariosa[.]baniosnaza[.]net/activates/?em=asdacz",	"http://clicktrackingsall[.]com/a[.]php",
"https://dinna-fashion[.]ru/d/mime[.]com/cast/next[.]php",	"https://www[.]myatharweiiect[.]com/CR/?xfsr=true",
"https://allmaart[.]com/wp-includes/images/path/mime[.]com/cast/",	"http://taas[.]fund[.]rewards-holders-erc20-tokens[.]com/myetherwallet[.]html?/access-my-wallet",
"http://www[.]marketier[.]info/admin/temp/surveys/1999/100/supp/pn/35fc9189402fb4ed149e6cca71a696ef/",	"http://mith[.]rewards-program-erc-20-token[.]com/myetherwallet[.]html?/access-my-wallet",

Siber Sözlük

NTP Protokolü:
NTP protokolü, internete bağlı olan cihazların saatlerini senkronize etmek için kullanılmaktadır.

Monlist Komutu:
Bu komut ile istekte bulunan makineye, sorgulanan sunucuya bağlanan son makinelerin listesi gönderilmektedir.

NTP Amplifikasyon:
NTP amplifikasyon saldırısı, DDOS saldırı türlerinden biridir. saldırganın NTP (Network Time Protocol) sunucularını kullanarak hedef sistemin bant genişliğini tüketmeye yönelik yapılır. Bu saldırılar yansıma saldırısı olarak da adlandırılır.

C&C:
Komuta ve kontrol merkezi. (Command and Control)

IOC:
Inversion of control, kontrolün tersine çevrilmesi yani tersine mühendislik için kullanılan yöntemleri ifade etmektedir.

Kurumumuza özel teknolojik çözümlerimiz
ile ilgili detaylı bilgi almak için
Türk Telekom satış yöneticiniz
veya 444 5 444 ile
iletişime geçebilirsiniz.

BU İŞTE BERABERİZ

Türk Telekom
Değerli Hissettirir